SEGURIDAD DE LA INFORMACIÓN EN LA INTERNET DE LAS COSAS

Cañon Miranda, David Alexander
davidcanon@hotmail.com
Universidad Piloto de Colombia

Abstract—The IoT has invaded every aspect of our lives, growing exponentially but as it grows in the quantity of uses and products, grows in flaws in its interfaces giving a negative expectation to security; steps towards a better security in the devices of the IoT had being taken but still there is a lack of consciousness from vendors as from users about information security to the level of interfaces as for connecting than for administration of the devices.

Index Terms— Arduino Boards, IoT, Internet of the things, M2M, Security.

Resumen—La IoT está invadiendo cada uno de los aspectos de nuestra vida, creciendo de manera exponencial, pero así como ésta crece en la cantidad de usos y productos crecen las falencias en sus interfaces, dando una expectativa negativa hacia la seguridad. Ya se han empezado a dar pasos en dirección a mejorar la seguridad en los dispositivos de la IoT pero falta conciencia de las empresas constructoras como de los usuarios con respecto a la seguridad de la información a nivel de las interfaces, tanto para conectarse como para administrar los dispositivos.

Índice de Términos — Arduino Boards, IoT, Internet de las cosas, M2M, Seguridad.

I. INTRODUCCIÓN

La Internet se ha expandido a todos los aspectos de nuestra vida, así no nos demos cuenta o parezca un tema de película de ciencia ficción, el futuro que vemos en estas películas ya está aquí y cada día tenemos más productos que se interconectan entre sí y a la Internet, hablando entre ellos y compartiendo información para hacer nuestra vida más fácil. Este ecosistema entre las "cosas" y la Internet es llamada la Internet de las cosas, antes nombrada como M2M (Machine To Machine).

Dé un vistazo por su casa. ¿Cuántos dispositivos se conectan a la Internet? El computador, la tableta y el celular, ¿y el televisor? Éste último es muy común, pero ya tenemos neveras, lavadoras, cafeteras, relojes de pulso y microondas, entre unos pocos que mencionar.

La IoT surge gracias a la convergencia de las nuevas tecnologías, donde tenemos dispositivos de bajo uso de energía y para usos personalizados como los nuevos Arduinos o ArduinoBoards y Raspberry PIs, estos son computadores miniatura con WIFI y/o Bluetooth a los que se le conectan sensores que toman datos y los informan de manera inalámbrica directamente a otros dispositivos o vía internet, estos son los cerebros de las cosas. Cada vez tenemos estas "cosas" más cerca de nosotros, además de tenerlas cerca las tenemos hablando entre ellas y con nosotros a través de la Internet, y no me refiero en nuestra casa, hablo de nuestros cuerpos, cosas como los relojes inteligentes y bandas que toman datos como nuestro pulso, pasos que hemos dado, y nuestra ubicación, llamados wearables (dispositivos que se usan puestos, que se pueden vestir para ser más fieles al significado de la palabra inglesa), además tenemos bombas de insulina con conexión Bluetooth, marcapasos con interfaces inalámbricas para poder ser monitoreados y configurados a las necesidades del paciente, y muchas más que ya están por ahí y no tardan en llegar.

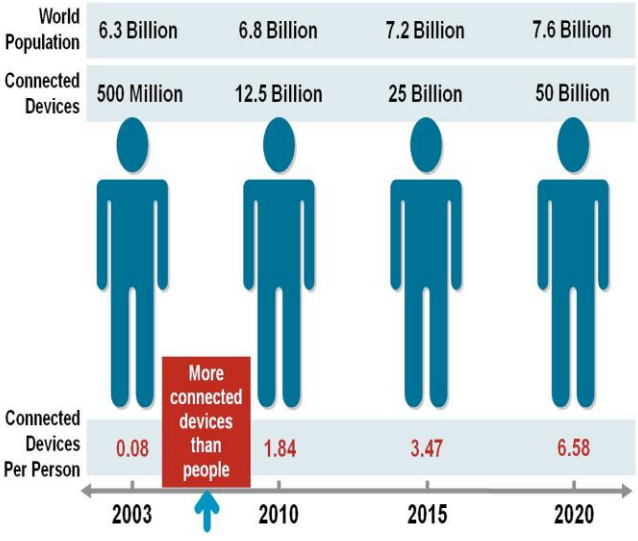
II. HISTORIA Y ESTADÍSTICAS DE LA IOT

La internet de las cosas lleva bastante tiempo en nuestras vidas, sin que nos diéramos cuenta o seamos consientes de ella, la historia de la IoT empieza para algunos desde la invención del telégrafo electromagnético en 1832 por el Barón Schilling en Rusia, y parte de esa historia temprana involucra a Nicola Tesla cuando en 1926 habló en una entrevista a cerca de lo inalámbrico, diciendo:

"Cuando lo inalámbrico sea perfectamente aplicado, el mundo entero se convertirá en un gran cerebro, el cual de hecho es, todas las cosas siendo partículas de un todo real y armonioso… y los instrumentos por medio de los cuales nosotros seremos capaces de hacer esto serán sorprendentemente simples comparados con nuestro teléfono actual. Un hombre podrá cargar uno en el bolsillo de su chaleco."

El término "Internet of Things" fue acuñado en 1999 por Kevin Ashton director ejecutivo de Auto-ID en una presentación sobre RFIDs para llamar la atención de la audiencia sobre estos y la internet. Se tiene como nacimiento de la IoT los años 2008 y 2009 porque es cuando se conectaron más cosas u objetos a la internet que personas según Cisco Internet Business Solutions Group y desde entonces cada vez más y más dispositivos hablan entre sí por la internet enviado información para evaluar y de estas evaluaciones llevar a cabo tareas que pueden ser triviales, hasta tareas de vida o muerte como cantidades de insulina a ser inyectadas en el organismo de alguna persona diabética. (Ver Gráfica I).

GRÁFICA I
THE INTERNET OF THINGS WAS "BORN" BETWEEN 2008 AND 2009



La IoT se introdujo al ciclo de impulso de Gartner en 2011, mostrando que tiene entre 5 y 10 años para ser adoptado por el público en general, es decir que dentro de los próximos años todos tendremos y usaremos alguno de estos dispositivos sepámoslo o no. (Ver Gráfica II).

GRÁFICA II
GARTNER HYPE CYCLE 2011

De acuerdo a Gartner la expectativa de cosas conectadas a la Internet para este año es 30% más que las del año pasado, y de casi un 400% más para el 2020, esto representa una suma proporcional en dinero invertido en la IoT, ya que a la par están convergiendo en el tiempo lo social, la nube, lo móvil y la información impulsados por la IoT. (Ver Tabla I).

TABLA I
GARTNER IOT UNIDADES INSTALADAS POR CATEGORÍA

Table 1: Internet of Things Units Installed Base by Category

Category	2013	2014	2015	2020
Automotive	96.0	189.6	372.3	3,511.1
Consumer	1,842.1	2,244.5	2,874.9	13,172.5
Generic Business	395.2	479.4	623.9	5,158.6
Vertical Business	698.7	836.5	1,009.4	3,164.4
Grand Total	**3,032.0**	**3,750.0**	**4,880.6**	**25,006.6**

Source: Gartner (November 2014)

III. ANTECEDENTES

Para aproximar más al público frente al tema de la IoT a continuación darermos una mirada de algunos casos que permitirán visualizar qué tan cerca estamos en estos momentos de esta realidad de la IoT.

En 2012 un investigador de McAffee logró acceder de manera ilícita a una bomba de insulina e hizo que esta dispensará las 300 unidades que contiene en una sola dosis, esto gracias a señales inalámbricas que se usan para comunicarse con el dispositivo, los investigadores dijeron que podían influenciar cualquier bomba de insulina en un rango de 100

metros a la redonda haciendo que dispensara una dosis letal [4]. Los dispositivos médicos en general son más susceptibles a ser accedidos de manera ilícita, ya que no se centran en la forma en que se pueden vulnerar como en su utilidad, se enfocan en el beneficio que estos pueden dar a nivel de la salud pero todo lo demás parece quedar en un segundo plano. Estos dispositivos al ayudar al soporte vital de las personas pueden llegar a ser usadados como armas causando daños en sus portadores y hasta la muerte, algunos puntos clave con respecto a estas vulnerabilidades son:

- Base de datos de problemas de los dispositivos sin información relevante a temas de seguridad.
- Falta de parcheo de dispositivos y computadores de hospitales debido a que los distribuidores pueden no dar soporte si se han cambiado las configuraciones originales de los dispositivos o computadores por perdidad de la garantia al ser modificadas. Además provocando que los dispositivos sean más vulnerables con el tiempo al poderse encontrar nuevas falencias y que estas no se pueden parchar.
- Los médicos involucrados en la toma de decisión de compra de equipos no tienen las bases tecnicas para hacer preguntas sobre la seguridad de estos, además las áreas de TI de las empresas que adquieren dichos dispositivos casi nunca participan en el proceso de compra, haciendo que el aspecto técnico a evaluar sea menor, así las pruebas se enfocan en temas mas funcionales sin ahondar en temas como las seguridad y las vulnerabilidades posibles.
- Los dispositivos médicos están más conectados a la red, pero la seguridad de los mismos no es acorde a este crecimiento que en los úlitmos años se ha visto en aumento [5].

Los carros inteligentes que están llegando al mercado ya han sido atacados por hackers de sombrero blanco demostrando espeluznantes ataques, cosas como dejar el auto sin frenos, hacer que frene a alta velocidad, disparar los airbags o cosas menos aterradoras como mostrar el medidor de gasolina lleno cuando no lo está, ajustar los cinturones de seguridad o hacer que los luces parpadeen. Una de estas demostraciones la hizo un niño de 14 años con solo 15 dólares en su bolsillo, el logró violar el sistema de un auto y hacer varios trucos como reproducir música y encender el vehículo de manera remota, ¿se imaginan lo que alguien con mas recursos, conocimiento y malas intesiones puede lograr?, lo que muestra que no se necesitan ingenieros con altos conocimientos, demostrando que la seguridad en estos sistemas es muy pobre, porque al igual que en los dispositivos médicos se enfocan en los temas funcionales y no en mejorar la seguridad de los dispositivos contraladores [6].

La vulnerabilidad de las “cosas” es evidente en todas las marcas, incluyendo los gigantes orientales. En el mes de agosto de 2015 se logró identificar una falencia en el sistema con el que se sincroniza una nevera inteligente, siendo esta una falla en las validaciones de SSL, permitiendo que se pueda robar las credenciales con las que se configura, en éste caso usuarios y contraseña de Gmail [7].

IV. Conciencia sobre la seguridad en la IoT

La conciencia sobre la seguridad es fundamental para los usuarios, los que intervienen en la construcción del hardware y software y aquellos que distribuyen los productos de la IoT, para entender que la Internet involucra conectarse con el mundo en dos vías, tanta para ver el exterior, como para mirar dentro de nuestras vidas, exponiéndonos a un vasto universo de personas con buenas y malas intensiones.

Por la globalización y el afán competitivo de las empresas se ha abierto una gran brecha de seguridad, la cual cada vez es más grande, el afán de llevar más dispositivos a los consumidores ha hecho que se descuiden aspectos básicos de la seguridad, por lo que debemos empezar a blindarnos para protegernos, evaluar a conciencia los dispositivos que usamos, tratar de documentar y estar seguros de las beneficios, de qué manera nos podemos estar exponiendo, es importante leer las letra pequeña, por ejemplo los televisores inteligentes que usan cámaras para ser manejados por gestos o por comandos de voz, dentro de la letra pequeña estos nos informan sobre las conversaciones que incluyan información personal o sensible, que dicha información estará entre la información capturada y trasmitida a terceros a

través del uso del *Reconocimiento de Voz* [8].

Una de las mayores dificultades que trae la IoT es la gran variedad de sistemas y protocolos que interactúan en las cosas que se conectan a Internet, por lo que se debe buscar un estándar que ayude a hacer un sistema seguro y dispositivos más compatibles, que hablemos un mismo "idioma" en lo que a esto respecta para poder halar en una misma dirección.

En relación a la compatibilidad se tienen grupos como "Internet of Things International Forum" y "The Internet of Things World Forum" [9] que apuntan a la compatibilidad pero no a la seguridad real del entorno de los dispositivos, estos tienen sistema operativos muy básicos, hechos pensando solamente en su función principal sin dar relevancia a cuestiones como el cifrado y la seguridad.

En las empresas se tiene un nuevo ámbito para la seguridad, los dispositivos que se conectan a sus redes internas como las bandas de control del estado físico (fitness bands) y relojes inteligentes (smart watches), los cuales envían y guardan información, son nuevos puntos de acceso al entorno de la empresa donde se puede comprometer la información sensible del negocio y de los clientes. La IoT es algo que no hace parte de la conciencia de empleados ni de directivos, pero sí de los cibercriminales. Negarnos al uso de estos dispositivos no es la solución, negarse a la IoT es rezagarse frente a los competidores, la IoT puede mejorar el negocio, la respuesta es la administración del riesgo. No esperemos que los fabricantes informen de sus vulnerabilidades, tampoco esperemos que ellos concienticen a los usuarios finales, ya que no toda la responsabilidad recae en los fabricantes, es importante que las áreas de TI tengan conciencia de los dispositivos que están conectados a las redes de su organización. Lo que las empresas pueden hacer es implementar mejores prácticas y estándares que se amolden a sus propias necesidades, se pueden tener en cuenta los siguientes puntos:

- Concientizar y educar a los directivos sobre las nuevas tecnologías el papel de la administración del riesgo.
- Asegurar que todos los dispositivos de la compañía que están en el lugar de trabajo estén actualizados.
- Exigir que los dispositivos de los empleados se conecten a las redes inalámbricas de invitados.
- Dar educación sobre ciberseguridad a los empleados para concientizarlos de las mejores prácticas y de los diferentes tipos de ataques.
- Asegurarse que los profesionales de TI y seguridad de la información estén certificados [10].

La seguridad de la tecnología como está concebida se basa en perímetros en estos momentos usamos VPNs y cortafuegos, pero ahora el perímetro se está ampliando, el área de cobertura de la IoT no tiene un límite claro ya que cada dispositivo se conecta de una manera diferente y expone y comparte la información a su manera, por lo que es más complicado asegurarlo. Debido a lo anterior, nos debemos valer del uso de las mejores prácticas, modelos de seguridad y recomendaciones mínimas para aplicarlas a nuestras redes y dispositivos.

Pensemos un poco en el software y como los desarrolladores deben comprometerse con la seguridad y no solo con la funcionalidad, ya que la información del cliente es igual de importante que la tarea que cumple la aplicación, un compromiso como el juramento Hipocrático que imponga una base ética, social y moral, en esta dirección apunta "The Rugged Manifesto" que traduce algo así como el manifiesto de fortaleza, donde se plasma el deseo de hacer códigos seguros y la responsabilidad que se tiene en el momento de desarrollarlos. El manifiesto da un aproximación para que las cosas se realicen bien hechas y con seguridad, imprimiendo y recordando que la ética en el trabajo no es algo tan simple como hacer un trabajo en tiempo o ajustarse a lo netamente funcional, es ir un poco más allá asegurando lo que a las personas les importa más que lo funcional y no entienden como puede ser revelado a terceros, de igual forma ya se viene trabajando en las mejoras prácticas en OWASP el cual tiene el "Internet of Things Top Ten Project" que busca ayudar a que todos tengan un mejor entendimiento sobre los asuntos de seguridad asociados a la IoT, y permite que los usuarios en cualquier contexto tomen las mejores decisiones sobre la seguridad cuando estén construyendo, desplegando o evaluando tecnologías

de la IoT.

En cada uno de los diez puntos principales que expone el OWASP como críticos para la IoT se hacen tres evaluaciones, la primera toma un grupo de factores que son: agentes de amenaza, vectores de ataque, debilidades de seguridad, impactos técnicos e impactos de negocios. La segunda es un ítem de pruebas, donde se hace una pregunta relacionada a determinar sí es seguro el punto en evaluación, de igual forma se analizan un grupo de fallas y se dan unos cuantos ejemplos de ataques. En tercer lugar, se determina como asegurar el punto evaluado, se plantea otra pregunta enfocada en cómo ser menos vulnerables.

Los diez tópicos evaluados a los cuales se les aplica los tres pasos antes mencionados son:

1. Interfaces Web inseguras.
2. Autenticación/Autorización insuficiente.
3. Servicios de red inseguros.
4. Carencia de cifrado en el transporte de datos.
5. Problemas de privacidad.
6. Interfaz con la nube insegura.
7. Interfaz móvil insegura.
8. Configuración de seguridad insuficiente.
9. Software/Firmware inseguro.
10. Pobre seguridad física.

La idea es cubrir toda la "superficie" de los dispositivos que hacen parte de la IoT para poder tener una mejor valoración de seguridad [11].

El más nuevo ente creado para tratar de asegurar la Internet de las cosas es "Internet of Things Security Foundation", conformado por más de 30 fabricantes entre ellos los grandes como Intel y Vodafone, ésta fundación se ha creado para tratar por medio de la educación de mejorar todos estos dispositivos, y de ésta manera cuidar la información de los clientes, la cual se ha visto expuesta con el acelerado crecimiento de las IoTs, esta iniciativa busca que personas y empresas no se alejen de las IoTs, haciendo de estas elementos más confiables para el consumo [12]. Asegurando un paso en la dirección correcta para tratar de corregir lo que se viene para el futuro, pero no olvidemos que la actualidad ya está inundada de "cosas" que son vulnerables, y que pueden exponernos a amigos indeseables, no entremos en pánico pero tampoco bajemos la guardia, tenemos que encontrar un equilibrio entre nuestros dispositivos y nuestra vida privada y de empresa.

V. Conclusiones

La IoT ha llegado para quedarse, estamos en la parte inicial de la cresta de esta gran revolución, y seguro ella hará mejor nuestras vidas, pero debemos tomar conciencia tanto como usuarios y oferentes de servicios que la seguridad es una necesidad y un derecho, el cual resguarda la privacidad e integridad de todos.

Existen muchos ejemplos de cómo las cosas de la IoT pueden llegar a manipularse de maneras maliciosas, y de que tenemos una gran oportunidad para mejorar.

Debemos abrazar las experiencias pasados y los conocimientos ganados, teniendo como base las mejores prácticas y el sentido común asegurando la integridad, disponibilidad y confidencialidad de la información en la IoT.

Referencias

[1] Gráfica I. https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[2] Gráfica II. http://postscapes.com/internet-of-things-added-to-the-2011-hype-cycle.

[3] Tabla I. http://diarioti.com/las-5-claves-principales-para-la-seguridad-en-internet-de-las-cosas/76218/.

[4] Can Your Insulin Pump Be Hacked? http://abcnews.go.com/blogs/health/2012/04/10/can-your-insulin-pump-be-hacked/.

[5] Hacking Insulin Pumps And Other Medical Devices From Black Hat http://www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other-medical-devices-reality-not-fiction/.

[6] Hackers Reveal Nasty New Car Attacks http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/, 14-Year-Old Hacks Connected Cars With Pocket Money http://www.forbes.com/sites/leoking/2015/02/23/14-year-old-hacks-connected-cars-with-pocket-money/.

[7] Robar contraseñas de GMail con un refrigerador, http://blog.segu-info.com.ar/2015/08/robar-contrasenas-de-gmail-con-un.html.

[8] Samsung's warning: Our Smart TVs record your living room chatterhttp://www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/.

[9] http://iotforum.org/ , https://www.iotwf.com/.

[10] Internet of Things Security Issues Require a Rethink on Risk Management,

http://blogs.wsj.com/cio/2015/10/14/internet-of-things-security-issues-require-a-rethink-on-risk-management/.
[11] OWASP Internet of Things Top Ten Project https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project.
[12] Smart devices to get security tune-up, http://www.bbc.com/news/technology-34324247.

Autor

David Alexander Cañon
Ingeniero de Sistemas
2004